

設定方法_①管理用通信を無効化

- 1 GUIでの設定方法
 - 1.1 作業対象のSNIPを確認
 - 1.2 SNIPの編集画面を開く
 - 1.3 SNIPの詳細設定を確認
 - 1.4 SNIPのmanagement accessを無効化
 - 1.5 無効化設定の確認 1
 - 1.6 無効化設定の確認 2
 - 1.7 設定の保存
- 2 CLIでの設定方法
 - 2.1 作業対象のSNIPを確認
 - 2.2 SNIPの詳細設定を確認
 - 2.3 SNIPのmanagement accessを無効化
 - 2.4 無効化設定の確認 1
 - 2.5 無効化設定の確認 2
 - 2.6 設定の保存
- 3 改訂履歴

GUIでの設定方法

以下操作は、NetScalerに対しhttpもしくはhttpsでログインした場合の設定方法を記載します。

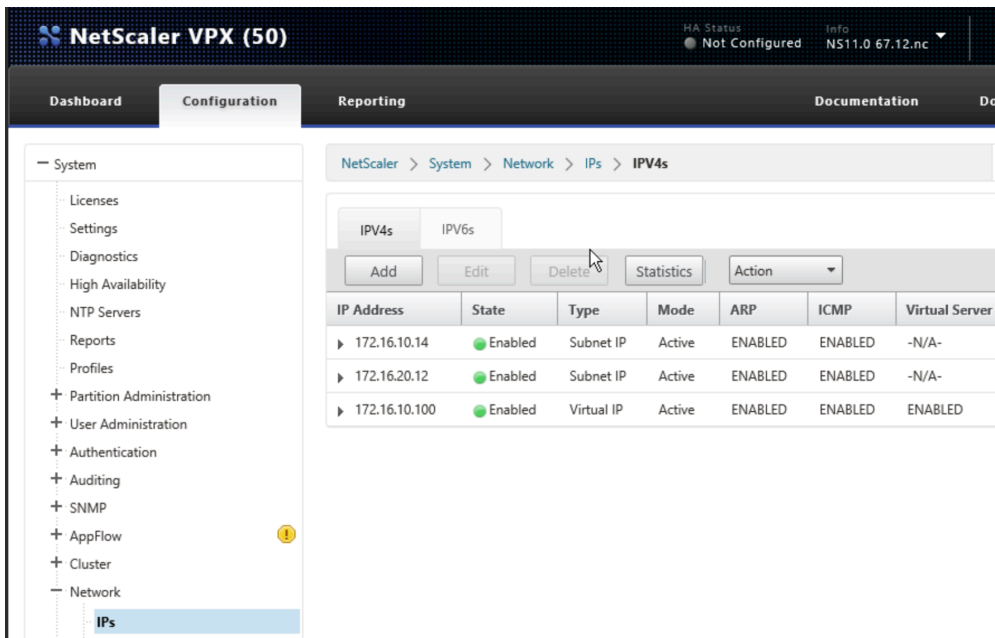
作業対象のSNIPを確認

System>Network>IPsに画面遷移し、NetScalerに登録されているIPアドレスを確認します。

TypeがSNIPとなっているアドレスのうち、設定変更が必要なアドレスがあることを確認ください。

以下の例では172.16.10.14及び172.16.20.12がSNIPであることがわかります。

以降の手順では、172.16.20.12が対処すべき対象として設定変更を進めます。



SNIPの編集画面を開く

変更したいSNIPを選択し、[Edit]ボタンを押下します。

The screenshot shows the NetScaler Configuration page. The left sidebar contains a tree view with 'System' expanded, showing 'Licenses', 'Settings', 'Diagnostics', 'High Availability', 'NTP Servers', 'Reports', 'Profiles', and 'Network'. Under 'Network', 'IPs' is selected. The main content area shows the 'IPV4s' configuration page. At the top, there are tabs for 'IPV4s' and 'IPV6s'. Below the tabs are buttons for 'Add', 'Edit', 'Delete', 'Statistics', and an 'Action' dropdown. A table lists the configured IP addresses:

IP Address	State	Type	Mode	ARP	ICMP	Virtual Server
▶ 172.16.10.14	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-
▶ 172.16.20.12	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-
▶ 172.16.10.100	Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED

The screenshot shows the NetScaler VPX (50) Configuration page. The left sidebar is identical to the first screenshot, with 'IPs' selected under 'Network'. The main content area shows the 'IPV4s' configuration page. At the top, there are tabs for 'IPV4s' and 'IPV6s'. Below the tabs are buttons for 'Add', 'Edit', 'Delete', 'Statistics', and an 'Action' dropdown. A table lists the configured IP addresses:

IP Address	State	Type	Mode	ARP	ICMP	Virtual Server
▶ 172.16.10.14	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-
▶ 172.16.20.12	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-
▶ 172.16.10.100	Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED

SNIPの詳細設定を確認

編集画面を下にスクロールしていくと、"Application Access Controls"欄が表示されます。

以下の例では、Enable Management Access、SSH、GUI、SNMPの4つがチェック(有効化)されていることがわかります。

☒ DYNAMIC_ROUTING ☐ RISE

Application Access Controls

☒ Enable Management Access control to support the below listed applications.

<input type="checkbox"/> Telnet	<input type="checkbox"/> FTP
<input checked="" type="checkbox"/> SSH	<input checked="" type="checkbox"/> SNMP ?
<input checked="" type="checkbox"/> GUI	<input type="checkbox"/> Secure Access Only
<input type="checkbox"/> Allow access only to management applications	

OK **Close**

SNIPのmanagement accessを無効化

有効化されているオプションに対し、**チェックを全て外します**。

以下の例は、SSH、GUI、SNMPのチェックを外し、最後に"Enable Management Access"のチェックを外すところを示します。

Application Access Controls

☒ Enable Management Access control to support the below listed applications. ?

<input type="checkbox"/> Telnet	<input type="checkbox"/> FTP
<input type="checkbox"/> SSH ?	<input type="checkbox"/> SNMP
<input type="checkbox"/> GUI	<input type="checkbox"/> Secure Access Only
<input type="checkbox"/> Allow access only to management applications	

OK **Close**



確実にオプションを無効化するため、チェックを外す順番は"Enable Management Access"以外から実施することをお勧めします。

"Enable Management Access"のオプションを外す際、確認のポップアップが出ますので[Yes]を選択ください。

Confirm

? This IP will not support applications like Telnet, FTP etc. if you disable Management Access.
Are you sure you want to proceed?

Yes **No**

"Application Access Controls"欄が以下のように縮小表示され、チェックが外れていることを確認したのち、[OK]を押下します。

Virtual Server RHI Mode

☒ DYNAMIC_ROUTING ☐ RISE

Application Access Controls

☐ Enable Management Access control to support the below listed applications.



お客様が設定変更を行うためにアクセスしているSNIPに対して上記を実施しますと、ログインができなくなります。

まだ設定は保存されておりませんので、ECL2.0カスタマーポータルからNetScalerを再起動するなどして変更前の状態に戻すことができます。

無効化設定の確認 1

設定変更したSNIPを再度選択し、[Edit]ボタンを押下します。

Dashboard Configuration Reporting Documentation Downloads

System

- Licenses
- Settings
- Diagnostics
- High Availability
- NTP Servers
- Reports
- Profiles
- + Partition Administration
- + User Administration
- + Authentication
- + Auditing
- + SNMP
- + AppFlow
- + Cluster
- Network
 - IPs

NetScaler > System > Network > IPs > IPV4s

IPV4s IPV6s

Add Edit Delete Statistics Action

IP Address	State	Type	Mode	ARP	ICMP	Virtual Server
▶ 172.16.10.14	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-
▶ 172.16.20.12	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-
▶ 172.16.10.100	Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED

"Application Access Controls"欄が以下のように縮小表示され、チェックが外れていれば無効されています。

Virtual Server RHI Mode

☒ DYNAMIC_ROUTING ☐ RISE

Application Access Controls

☐ Enable Management Access control to support the below listed applications.

無効化設定の確認 2

無効化を実施したSNIPに対し、NetScalerの外部からssh、gui(http、https)でのログイン、snmpでの値取得を試み応答が返ってこないことを

確認ください。

お客様の環境に依存するため、例は載せておりません。

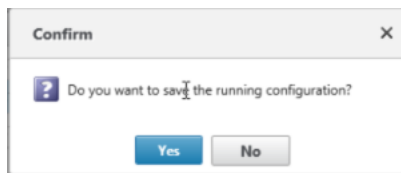
設定の保存

画面右上にフロッピーディスクのマークを押下します。



IP Address	State	Type	Mode	ARP	ICMP	Virtual Server	Traffic Domain
▶ 172.16.10.14	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-	10
▶ 172.16.20.12	Enabled	Subnet IP	Active	ENABLED	ENABLED	-N/A-	10
▶ 172.16.10.100	Enabled	Virtual IP	Active	ENABLED	ENABLED	ENABLED	10

確認のポップアップが出ますので[Yes]を選択ください。



本操作を実施しない場合、何らかの理由でNetScalerが再起動した際に変更した設定が全て元の状態に戻ります。
必ず設定を保存するようご注意ください。

CLIでの設定方法

以下操作は、NetScalerに対しsshでログインした場合の設定方法を記載します。

作業対象のSNIPを確認

```
show ns ip
```

を実行し、NetScalerに登録されているIPアドレスを確認します。

TypeがSNIPとなっているアドレスのうち、設定変更が必要なアドレスがあることを確認ください。

以下の例では172.16.10.14及び172.16.20.12がSNIPであることがわかります。

以降の手順では、172.16.20.12が対処すべき対象として設定変更を進めます。

```
> show ns ip
Ipaddress      Traffic Domain Type      Mode  Arp  Icmp  Vserver State
-----
1) 172.16.10.14  10          SNIP    Active Enabled Enabled NA    Enabled
2) 172.16.20.12  10          SNIP    Active Enabled Enabled NA    Enabled
3) 172.16.10.100 10          VIP     Active Enabled Enabled Enabled Enabled
Done
```

SNIPの詳細設定を確認

```
show ns ip "対象のIPアドレス" -td 10
```

を実行し、management access及びsshなどのオプション状況を確認します。

以下の例では、management access、ssh、gui、snmpがEnabledになっていることがわかります。

```
> show ns ip 172.16.20.12 -td 10
IP: 172.16.20.12
(中略)
management access: Enabled
telnet: Disabled
ftp: Disabled
ssh: Enabled
gui: Enabled
snmp: Enabled
(中略)
Done
```

SNIPのmanagement accessを無効化

対象のIPアドレスでEnabledになっていたmanagement access及びsshなどのオプションを下記コマンドで無効化(Disabled)します。

```
set ns ip "対象のIPアドレス" -td 10 -ssh Disabled -gui Disabled -snmp Disabled -mgmtAccess Disabled
```

以下の例では、172.16.20.12に対して、management access、ssh、gui、snmpをDisabledに変更しています。

```
> set ns ip 172.16.20.12 -td 10 -ssh Disabled -gui Disabled -snmp Disabled -mgmtAccess Disabled
Done
```



お客様が設定変更を行うためにアクセスしているSNIPに対して上記コマンドを実施しますと、再びログインができなくなります。

まだ設定は保存されておきませんので、ECL2.0カスタマーポータルからNetScalerを再起動するなどして変更前の状態に戻すことができます。

無効化設定の確認 1

```
show ns ip "対象のIPアドレス" -td 10
```

を実行し、management access及びsshなどのオプション状況を確認します。

以下の例では、management access、ssh、gui、snmpが全てDisabledになっていることがわかります。

```
> show ns ip 172.16.20.12 -td 10
IP: 172.16.20.12
(中略)
management access: Disabled
telnet: Disabled
ftp: Disabled
ssh: Disabled
gui: Disabled
snmp: Disabled
(中略)
Done
```

無効化設定の確認 2

無効化を実施したSNIPに対し、NetScalerの外部からssh、gui(http、https)でのログイン、snmpでの値取得を試み応答が返ってこないことを確認ください。

お客様の環境に依存するため、例は載せておりません。

設定の保存

```
save ns config
```

を実行し、変更した設定を保存下さい。



本操作を実施しない場合、何らかの理由でNetScalerが再起動した際に変更した設定が全て元の状態に戻ります。

必ず設定を保存するようご注意ください。

改訂履歴

日付	版数	変更点
2017/9/27	1.0.0	初版